



CITY OF OAKLAND

AGENDA REPORT

TO: Jestin D. Johnson
City Administrator

FROM: Darren Allison
Interim Chief of Police

SUBJECT: OPD Surveillance Technology 2022
Annual Reports

DATE: August 15, 2023

City Administrator Approval 

Date: Sep 13, 2023

RECOMMENDATION

Staff Recommends That The City Council Receive An Informational Report of Oakland Police Department's Surveillance Technology 2022 Annual Reports.

EXECUTIVE SUMMARY

This informational report includes OPD surveillance technology annual reports, which have been reviewed and approved by the Privacy Advisory Commission. These include Mobile ID, Live Stream Camera Systems, Cellular Site Simulator, Unmanned Aerial System (UAS)/Drones, ShotSpotter, Biometric Crime Lab, StarChase/GPS Tag Tracker, and Forensic Logic Coplink.

BACKGROUND / LEGISLATIVE HISTORY

[Oakland Municipal Code \(OMC\) 9.64.040](#): Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for the Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs, and civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

ANALYSIS AND POLICY ALTERNATIVES

This report advances the Citywide priorities of holistic community safety and responsive, trustworthy government. Surveillance technology is used to help OPD respond in a more timely and efficient manner in public safety concerns. OPD strives to use technology in a responsible manner by following the departmental use policies and by bringing the reports to PAC in a timely manner each year.

Please see each attachment for complete information. These include: Mobile ID (**Attachment A**), Live Stream (**Attachment B**), Cellular Site Simulator (**Attachment C**), Unmanned Aerial System

Public Safety Committee
September 26, 2023

(UAS)/Drones (**Attachment D**), ShotSpotter (**Attachment E**), Biometric Crime Lab (**Attachment F**), StarChase/GPS Tag Tracker (**Attachment G**), and Forensic Logic Coplink (**Attachment H**).

FISCAL IMPACT

Please see each attachment for complete information.

PUBLIC OUTREACH / INTEREST

No outreach was deemed necessary for the proposed policy action beyond the standard City Council agenda noticing procedures. However, each report details if community outreach was needed or if community feedback was received about the technology.

COORDINATION

These reports were scheduled to the Privacy Advisory Commission agenda. PAC reviewed, discussed, and approved all of these reports.

SUSTAINABLE OPPORTUNITIES

Economic: Please see each attachment for complete information.

Environmental: Please see each attachment for complete information.

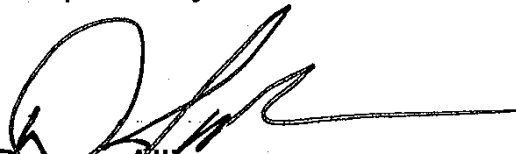
Race & Equity: OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is in compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

ACTION REQUESTED OF THE CITY COUNCIL

Staff Recommends That The City Council Receive An Informational Report of Oakland Police Department's Surveillance Technology Annual Reports.

For questions regarding this report, please contact David Elzey, Acting Deputy Chief, delzey@oaklandca.gov.

Respectfully submitted,



Darren Allison
Interim Chief of Police
Oakland Police Department

Reviewed by,
David Elzey, Acting Deputy Chief
OPD, Bureau of Investigations

Prepared by:
Tracey Jones, Police Services Manager
OPD, BOS, Research and Planning Unit

David Pullen, Officer
OPD, Bureau of Services, Information Technology Unit

Attachments (8):

- A: Mobile ID annual report
- B: Live Stream
- C: Cellular Site
- D: UAS/Drones
- E: ShotSpotter report and attachments
- F: Biometric Crime Lab
- G: StarChase/GPS Tag Tracker
- H: Forensic Logic Coplink

Attachment A: Mobile ID

Background

The City Council adopted [Resolution 88095 C.M.S.](#) on April 7, 2020, which approved the OPD Mobile ID Surveillance Use Policy as well as the Surveillance Impact Report.

OPD does not currently possess any Mobile Identification Devices (MID)s and there was zero (0) MID usage by OPD in 2022. The Alameda County Sheriff's Office (ACSO), the lead sponsor of the MID program, is currently upgrading the devices with technology provider. OPD will appoint an internal MID Coordinator when OPD is able to receive and deploy upgraded units.

2022 Annual Report Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

OPD did not possess nor deploy MIDs in 2022.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

There was no usage and no data generated in 2022.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

MIDs are not attached to any fixed objects.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

OPD did not deploy MIDs anywhere in the City in 2022.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

There were no community complaints or concerns.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

There was no usage of MIDs and no data or usage to audit.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no identifiable data breaches or unauthorized access during the year of 2022.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Non-applicable based on zero usage.

- I. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates:

There were no PRRs regarding this technology in 2022.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

There was no MID usage and no cost to OPD.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

Attachment B: Live Stream

Background

Oakland Police Department (OPD) I-23: Live Stream Transmitter Use Policy governs OPD's use of Live Stream Transmitters; the policy was approved by the City Council on April 21, 2020, through Resolution No. 88099 C.M.S., as well as OMC 9.64.040, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council. The information provided below is compliant with the annual report policy requirements of OMC 9.64.040 and DGO I-23.

Sergeant Ann Pierce is currently the Live Stream / Video Team Program Coordinator.

2022 Annual Report Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

OPD did not use the livestream transmitter technology in 2022.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

No data was collected with this technology in 2022.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The transmitters are attached to handheld video cameras. These cameras are physically held by officers when in use.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

The live stream transmitters were not deployed in 2022.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a

determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

This technology was not used in 2022.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

There was no usage of the technology in 2022.

- Technology was properly stored with the OPD Information Technology Unit (ITU).
- OPD is not aware of any policy violations from the use of the live stream transmitters in 2022.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no identifiable data breaches or unauthorized access during the year of 2022.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

N/A

- I. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates:

There were no PRRs regarding this technology in 2022.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

\$11,500 for cellular connectivity.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

Attachment C: Cellular Site Simulator

Oakland Police Department (OPD) Department General Order (DGO) I-11: Cellular Site Simulator (CSS) Usage and Privacy, requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the Public Safety Committee. The information provided below is compliant with these annual report requirements.

***The technology has reached its lifespan and is unusable. The company stopped building the machines.

2022 Annual Report Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

The Cell Site Simulator Surveillance (CSS) Impact report explains that, "Cellular site simulators, as governed by this policy, function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the simulator identify it as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would a networked tower.

CSS receives signals and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider to distinguish between incoming signals until the targeted device is located. Once the cellular site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone, rejecting all others.

The authorized purposes for using CSS interception technology and for collecting information using that technology are to:

- a. Locate missing persons*
- b. Locate at-risk individuals*
- c. Locate victims of mass casualty incidents*
- d. Assist in investigations involving danger to the life or physical safety of an individual*
- e. Apprehend fugitives*

The technology was not used in 2022.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

DGO I-11 does provide that OPD may share CSS data with other law enforcement agencies that have a right to know and a need to know¹, such as an inspector with the

¹ DGO I-11 explains that a right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law.

District Attorney's Office. However, no CSS data would be downloaded, retained, or shared. No data was generated or shared with any agency because it was not actually used in 2022.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

CSS is not attached to fixed objects.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year.

CSS was not utilized anywhere in the City in 2022.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information.

There were no uses in 2022, and thus no need for any audits. There were no policy violations.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no identifiable data breaches or unauthorized access during the year 2022.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Tech was not used in 2022.

- I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates.

There are no existing or new public records requests for the 2022 calendar year.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year.

Zero (\$0.00). OPD did not incur any maintenance, licensing, or training costs.

Attachment D: UAS/Drones

The PAC voted unanimously to recommend City Council adoption of OPD's Departmental General Order (DGO) I-25: Unmanned Aerial System (UAS) Use Policy on May 14, 2020. The City Council adopted Resolution No. 88454 C.M.S., which approved OPD's DGO I-25. OMC 9.64.040 requires that, after City Council approval, OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

Lieutenant Daza-Quiroz is currently the UAS Program Coordinator.

2022 Data Points

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

From the "Surveillance Impact Use Report for the Unmanned Aerial System (UAS)"

An Unmanned Aerial System (UAS) is an unmanned aircraft of any type that is capable of sustaining directed flight, whether preprogrammed or remotely controlled (commonly referred to as an unmanned aerial vehicle (UAV)), and all of the supporting or attached components designed for gathering information through imaging, recording, or any other means.

UAS is controlled from a remote-control unit (similar to a tablet computer). Wireless connectivity lets pilots view the UAV and its surroundings from a birds-eye perspective. UAV pilots can leverage control unit applications to pre-program specific GPS coordinates and create an automated flight path for the drone.

UAS have cameras so the UAS pilot can view the aerial perspective. UAS proposed for use by OPD and/or the Alameda County Sheriff's Office use secure digital (SD) memory cards to record image and video data; SD cards can be removed from UAS after flights to input into a computer for evidence.

UAS technology was used in the following ways/with the following outcomes in 2022:

One Hundred and Thirty-Two (132) uses. OPD responded to One Hundred and Nine (109) deployments and missions. Alameda County Sheriff's Office (ACSO) or neighboring agencies with UAS Programs responded to twenty-three (23) requests. Sometimes ACSO will offer their services prior to being requested². However, all agencies will only deploy if requested or approved by an OPD commander and if policy requirements are met. OPD Electronic Support Unit (ESU) has created a spreadsheet to track and monitor outside agency deployments. Lt. O. Daza-Quiroz sent a department wide email mandating all commanders who deploy drones to author documentation, similar to the protocol for the use of the Emergency Rescue / Armored Vehicles. This process has allowed for appropriate documentation.

Table 1 below details the deployments of OPD and ACSO Drones in 2022 in the City of Oakland

Table 1: 2022 OPD & ACSO Drone Deployments

² ACSO has access to OPD radio channels and can monitor; ACSO personnel at times can respond to a call for service.

Incident Type	OPD	ACSO	Total
Mass casualty incidents	0	0	0
Disaster management	1	0	1
Missing or lost persons	3	0	3
Hazardous material releases	0	0	0
Sideshow events	4	0	4
Rescue operations	4	1	5
Training	4	0	4
Barricaded suspects	16	7	23
Hostage situations	0	2(HPD)	2
Armed suicidal persons	0	0	0
Arrest of armed and/or dangerous persons	53	7	60
Scene documentation for evidentiary or investigation value	2	0	2
Operational pre-planning	0	0	0
Service of high-risk search and arrest warrants	22	0	22
Exigent circumstances	0	0	0
Total	109	23	132

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Twenty-Three (23) times. Outside Law Enforcement Agencies (ACSO, Hayward PD) assisted in 23 UAS deployments in Oakland in 2022. Because of this, the UAS aircraft that they used captured and stored data. These agencies provide OPD with the recordings and store the information in their logs per their respective policy requirements. No outside entity made any requests to OPD to share any of OPD's data acquired using OPDs UAS, nor did OPD share any data acquired through OPDs UAS with outside entities.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The technology was never installed upon fixed objects.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year

Table 2 below details the Police Areas where UAS were deployed in 2022.

Table 2: OPD UAS Deployment by Police Area

Deployment by Area	Total Deployments
Area 1	21
Area 2	8
Area 3	21
Area 4	26
Area 5	27
Area 6	24
Outside City*	5
Total*	132

* Deployments outside the city consist of assistance provided by OPD UAS to local agencies, or provided to assist OPD enforcement activities that took place outside the city of Oakland.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

Table 3 below provides race data related to 2022 UAS deployments.

Table 3: Race of Detainees Connected to OPD UAS Deployments in 2022

	Race – Female	Race - Male	Total
Black	27	81	108
Hispanic	16	42	58
Asian	0	13	13
White	4	4	8
Other	1	12	13
Total	48	152	200

OPD knows the race of detainees connected to UAS deployments. However, the race of all individuals involved in many UAS deployments is not known. There are cases such as barricaded suspects, where no suspect is ever discovered or detained. There could also be UAS uses for missing persons where the person's identity is not entirely known nor discovered.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information

The OPD Electronic Surveillance Unit (ESU) maintained a list of all UAS deployment logs for record and tracking purposes. This list was reviewed periodically for accuracy and for assessment of any policy violations. All OPD commanders were directed to send communications to ESU for any UAS request or use – similar to OPD protocols for the use of Emergency Rescue / Armored Vehicles. No policy violations were found, and no corrective actions were warranted nor needed in 2022.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no identifiable data breaches or unauthorized access during the year of 2022.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

In reviewing the data associated with UAS deployments, it was apparent that the unit has been effective at achieving safer outcomes for members of the community, officers, and those we have contacted during investigations.

During this review period OPD had over 100 deployments. Specific records were kept tracking the efficacy of those deployments with the following results:

- During a deployment, there was about a 75% chance of a subject being located. Nearly half of those deployments were for potentially armed and/or dangerous subjects.
- As a result, over 140 subjects were located by the UAS, and this resulted in about 76 arrests.
- 65 firearms were recovered when UAS was deployed in 2022.
- The Entry Team (SWAT Team) saw a decrease in Blue Alert deployments. In 2023 there has only been one Entry Team deployment at the time this report was authored. This decrease in deployments represents reduced emotional trauma to the community and significant fiscal savings for the city.
- Canine deployments were reduced by nearly 20%.

Over 60 of the deployments were for persons who were considered armed and/or dangerous. Because of the ability to deploy UAS, responding emergency personnel were better able to create an environment of de-escalation. Absent the UAS, officers would typically resort to calling out the Entry Team, deploying a canine, or physically clearing the area with a search team for the subject(s). All of these options have the potential for chance encounters resulting in the possibility of force escalation. These options decrease safety for the officers and the subjects of our contacts.

A sample below outlines just a few of the successful UAS deployments that provided officers increased safety and conditions for de-escalation:

1. *Officers located an armed carjacking vehicle parked in the 1400 blk of Fruitvale Av. The suspect was asleep in the driver's seat, and it was unknown if he was currently armed. UAS were deployed as overwatch, and one suspect was taken into custody. 23-002487*
2. *Officers responded to a report of multiple gunshots heard in the area. Officers recognized the location from the previous incident. Officers were advised by a community member that the person at this location was seen shooting guns. Officers observed the suspect exiting the location while wearing a bulletproof vest, who was then detained. A security sweep was conducted, and 16 firearms and over 100 spent casings were located. 23-001708.*
3. *OPD Ceasefire units conducted a stop on a driver of a stolen vehicle believed to be involved in a recent carjacking. A second suspect barricaded himself inside of a hotel room. A Surround and Call Out protocol was initiated, and a search warrant was obtained for a search of the room. Although the suspect was GOA, the suspect's clothing and a firearm were located in the room. 23-003067*
4. *Officers responded to a shot spotter activation. During the course of the preliminary investigation, officers determined that a shootout occurred, and one of the parties fled inside REDACTED 85th Ave. A surround and callout was initiated. Numerous individuals were detained, and a firearm was recovered. 23-005620*
5. *CID Officers were conducting an investigation when they were shot at with a firearm. Argus followed the suspect, in which one suspect ran into REDACTED Delaware Ave. UAVs were deployed to search the residence for the suspect. 1 suspect was located and placed under arrest. 23-008000*

As UAS deployments increase in response to demands from the City, we expect continuous positive outcomes from the use of this technology.

- I. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates.

There was only 1 Drone PRR (PRR 22-3024) request in 2022.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year

The UAS unit currently has ten members. These members engage in 240 hours of training annually to ensure compliance with Department policy and FAA regulations. The member's training is conducted during their regular scheduled shifts minimizing costs. Adjusting for top rate salary, the training is estimated to cost \$158,327.00 for 2023 and will be paid for by the Department.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request.

No requests for policy changes at this time.

Attachment E: ShotSpotter

The PAC recommended adoption of OPD Department General Order (DGO) I-20: “Gunshot Location Detection System” at their October 3, 2019, meeting; the report was presented to the City Council on November 19, 2019, and adopted by the City Council via Resolution No. 87937 C.M.S. DGO I-20 requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

2022 Data Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

From the “Surveillance Impact Use Report for the Gunshot Location Detection System:”

Part 1 – How the System Works: “The GLD system sensors are designed to detect gunshots based on their acoustic signature (e.g., broad-frequency, impulsiveness, and loudness). The utilization of multiple sensors at different distances from a gunshot sound allows the system not only to capture the sound but also assign a probability that it is a gunshot and triangulate its precise location based on the time difference of arrival. If the machine classifier in the “ShotSpotter Cloud” determines it is likely a gunshot based on computer-learning algorithms, the system will pull a short audio snippet from the sensors that detected it and send it to human analysts at the ShotSpotter Incident Review Center at its headquarters in Newark, CA. The analysts perform an auditory and visual assessment of the audio waveform to make a final determination as part of a two-phased classification process. If confirmed as a gunshot, an alert is published containing information such as street address, number of rounds fired, and a short audio snippet of the gunfire event– all within 60 seconds of the trigger pull (29 seconds on average).”

From Section 2: Proposed Purpose: “The purpose of GLD is to enable OPD to provide a higher level of service to the community related to shootings. The system detects, locates, and alerts officers of virtually all gunshots in a coverage area in less than 60 seconds, enabling officers to respond to and investigate gunshot incidents they would not have known about and to respond to them much more rapidly than waiting for a 911 call. Personnel can better respond to gunshot activity and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data.”

ShotSpotter technology was used in the following ways/with the following outcomes in 2022:

- The number of times ShotSpotter technology was requested: ShotSpotter alerted OPD to 7,562 unique gunshot incidents from January 1 – December 31, 2022. Of those alerts, **7,481 (99%) were not called in by the community as a 415GS call type (shots fired)**, and OPD would not have known about them nor have been able to respond in a timely fashion. This information is based on an analysis of calls within 15 minutes and 1,000 feet of a ShotSpotter alert.
- ShotSpotter led police to **199 shooting cases, 28 of which were Homicide and 171 were Assault with a Firearm**. OPD was able to provide and coordinate immediate emergency medical response on these shooting cases; OPD personnel believe that several of these victims survived the shootings specifically because of the quick response and subsequent medical attention. In some instances, OPD and medical response occurred within less than two minutes of the ShotSpotter activation. The ShotSpotter alert was within 10 minutes and 1,000 feet of the location where the victim

was found. Furthermore, staff believe that there were many more cases where OPD responded to activations and found shooting victims – and where critical medical attention was provided. The 199 cases cited here (171 injury cases) are the ones where OPD and ShotSpotter staff can conclusively cite the response to the ShotSpotter activations.

- ShotSpotter activations led OPD to **162 cases where their vehicle and/or dwelling was hit by gunfire. Of these 162 cases, 71 victims were present but not hit by gunfire, and 91 were listed as victims because the property belonged to them.**
- 1,789 crime incident reports (24% of total activations)
 - 1,252 (70%) of these incidents resulted in OPD Crime Lab requests for further firearm forensic analysis.
- ShotSpotter provided the following additional reports in relation to specific ShotSpotter activations:
 - **Eleven detailed forensic reports**
 - **Court preparation for seven cases (*DA subpoenaed ShotSpotter for this information*)**
 - **Investigative Lead Summary 1,181**

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The following agencies have been provided log-in access to the ShotSpotter System for ongoing usage and do not make written requests for access:

OPD and the Oakland Housing Authority Police Department entered into a Memorandum of Understanding (MOU) in 2012, following City Council approval, to fund the initial ShotSpotter program in areas of the City and near OHA buildings known for higher levels of gunshots. This MOU allows OPD to share access to the ShotSpotter cloud-based portal with OHA PD personnel (see **Attachment C**).

DGO I-20 Section B – 1. “Authorized Use” (From Use Policy Approved by City Council November 19, 2019) states:

The Chief of Police or designee shall provide necessary training and/or technical assistance for GLD usage. Only OPD personnel shall be granted access to OPD’s GLD System. The GLD system shall only be used for locating gunshots. The system shall never be used to record human conversations except where such conversations are unintentionally recorded in connection with gunshot recordings.

DGO I-20 provides rules for sharing ShotSpotter System data with outside agencies. Section C–3 of DGO I-20: “GUNSHOT LOCATION DETECTION SYSTEM” – “Releasing or Sharing GLD System Data,” states:

“GLD system data may be shared only with other law enforcement or prosecutorial agencies based on a need to know or a right to know, or as otherwise required by law, using the following procedures:

1. The agency makes a written request for the ShotSpotter data that includes:
 - a. The name of the requesting agency.

- b. The name of the individual making the request.
 - c. The need for obtaining the information.
2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.
3. The approved request is retained on file and shall be included in the annual report.

There were no outside agency ShotSpotter data requests for OPD in 2022.

OPD investigators in the Criminal Investigations Division and or other sections of OPD, such as the Ceasefire Section and Violent Crime Operations Center, regularly communicate with personnel from other law enforcement agencies on inter jurisdictional investigations; these forms of collaboration may involve discussions related to shootings where OPD became informed from ShotSpotter activations. ShotSpotter activations many times may lead to evidence gathering (e.g., finding bullet casings); OPD may share information about evidence (e.g., that bullet casings were found in a particular area at a particular time). For prosecutorial purposes, OPD investigators may provide ShotSpotter data to be included with the investigative criminal case packet as relevant evidence to the District Attorney's Office as part of the case charging process and/or discovery.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

OPD has contracted with ShotSpotter to install GLD sensors in different areas (phases) in several parts of the city. The total coverage area for the current ShotSpotter system comprises 18.17 square miles, or approximately 32 percent of the city's land size (55.93). OPD has chosen to install the sensors in areas most prone to gunshots based on historical data. Many areas in East and West Oakland now benefit from the GLD system.

Most sensors are placed approximately 30 feet above ground level to maximize sound triangulation to fixed structures (e.g., buildings); at this altitude, the sensors can only record limited street-level human voice sounds. Furthermore, ShotSpotter only retains the audio for one second prior to a gunshot, and one second after.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

Attachment A to this report provides the geographic areas of the City of Oakland that comprise the three ShotSpotter "phases" or areas covered under the current OPD-ShotSpotter contract. These areas intersect with all six official OPD Police Areas with a focus on areas where gunfire has historically occurred with greater regularity. **Attachment B** to this report is a weekly public ShotSpotter Activation Report for the week; this later report highlights areas of Oakland where ShotSpotter alerts have most recently occurred.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each activation since shooting suspects are often unknown. Many times, there is data regarding the race of shooting victims or witnesses (may be self-reported); however, this data is not captured in the same system as ShotSpotter, and the administrative burden (7,562 total 2022 activations) to constantly connect the two disparate datasets would overwhelm staff capacity. OPD therefore recommends that the PAC makes the determination, that the administrative burden in collecting or verifying this information, as well as the associated potential for greater invasiveness in capturing such data, outweighs the benefit.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

New officers and crime analysts are trained on the ShotSpotter System as part of police officer academies. Officers and analysts are provided with directions that covers login, and how to use different views (e.g., time-period).

OPD officers have automatic access to ShotSpotter notifications when in patrol vehicles equipped with standard vehicle computers via the ShotSpotter Respond System. ShotSpotter creates a log for every sign-in to their system, which includes the level of access the user has (admin view or dispatch view, which is notification only). OPD and ShotSpotter have verified that for 2022, all users who logged into the system were authorized users.

Patrol Officers in vehicles and/or on mobile phones utilize the ShotSpotter Respond System. The Respond System pushes notifications to users – there is no interactivity functionality. ShotSpotter can only audit logins for both the Respond and the Insight programs. ShotSpotter and OPD staff have verified that all logins were associated with appropriate active employees. Staff regularly remove access from employee emails where staff separate from City employment.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no identifiable data breaches or unauthorized access during the year 2022.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 1: ShotSpotter Activations Resulting in Incident Report for Firearm Crimes by Category in 2022

Cases by Firearm-Related Crime Type	
Homicide	28
Assault with a Firearm	171
Shoot at an Occupied Home/Vehicle	71
Shoot at an Unoccupied Home/Vehicle	91
Negligent Discharge of a Firearm	1,363
Weapons Violations (including exhibit/draw)	11
Carjacking with a Firearm (including attempts)	4
Robbery with a Firearm (including attempts)	19
Total Cases	1,758

Table 2: Firearm Recoveries in 2022 Connected to ShotSpotter Activations Illustrate Guns Recovered

Guns Recovered by Crime Type	
Homicide	12
Assault with a Firearm	19
Shoot at an Occupied Home/Vehicle	2
Shoot at an Unoccupied Home/Vehicle	0
Negligent Discharge of a Firearm	38
Weapons Violations (including exhibit/draw)	9
Carjacking with a Firearm (including attempts)	1
Robbery with a Firearm (including attempts)	1
Other	1
Total Cases	83

- 83 weapons seized.
 - Note: More than one firearm may be from the same incident.
- 967 alerts when advanced situational awareness was provided to responding patrol officers on their way to crime scenes in high danger situations that required specific approach tactics such as multiple shooters, high capacity or automatic weapons being used, and drive-by shootings. Some of the alerts had more than one situational awareness tag amounting to 1,230 tags within those 967 alerts.

Table 4: Cases Where ShotSpotter Notifications Resulted in Firearm-Related Crimes

Cases by Firearm-Related Crime Type	
Homicide	28
Assault with a Firearm	171
Shoot at an Occupied Home/Vehicle	71
Shoot at an Unoccupied Home/Vehicle	91
Negligent Discharge of a Firearm	1,363
Weapons Violations (including exhibit/draw)	11
Carjacking with a Firearm (including attempts)	4
Robbery with a Firearm (including attempts)	19
Total Cases	1,758

I. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates:

There were 25 total PRRs in 2022. 20 are closed, and *4 remain open.

- 22-1338
- 22-2190
- 22-3599
- 22-3757
- 22-4463
- 22-5180
- 22-5665
- 22-6018
- 22-6019
- 22-6625
- 22-6900
- 22-6911
- 22-7134
- *22-7709
- *22-8250
- 22-8789
- 22-8850
- 22-9599
- 22-9600
- *22-9601
- *22-9602
- 22-9774
- 22-9775
- 22-9776
- 22-9777

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

The total paid in 2022 was \$798,486 for 18.17 square miles of coverage. These fees encompass all services ShotSpotter currently provides to Oakland. There are no additional charges for meetings, reports, analysis, and training. These funds come from OPD's General Purpose Fund.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for policy changes at this time.

Attachments for ShotSpotter Report

Phase I with red borders (Activated in 2006): 6.20 square miles*

East Oakland: East of High Street to 106th Avenue

West Oakland: East of Highway 980 to Frontage Road

Phase II with blue borders (Activated in 2013): 6.64 square miles

East Oakland: West of High Street to Park Boulevard

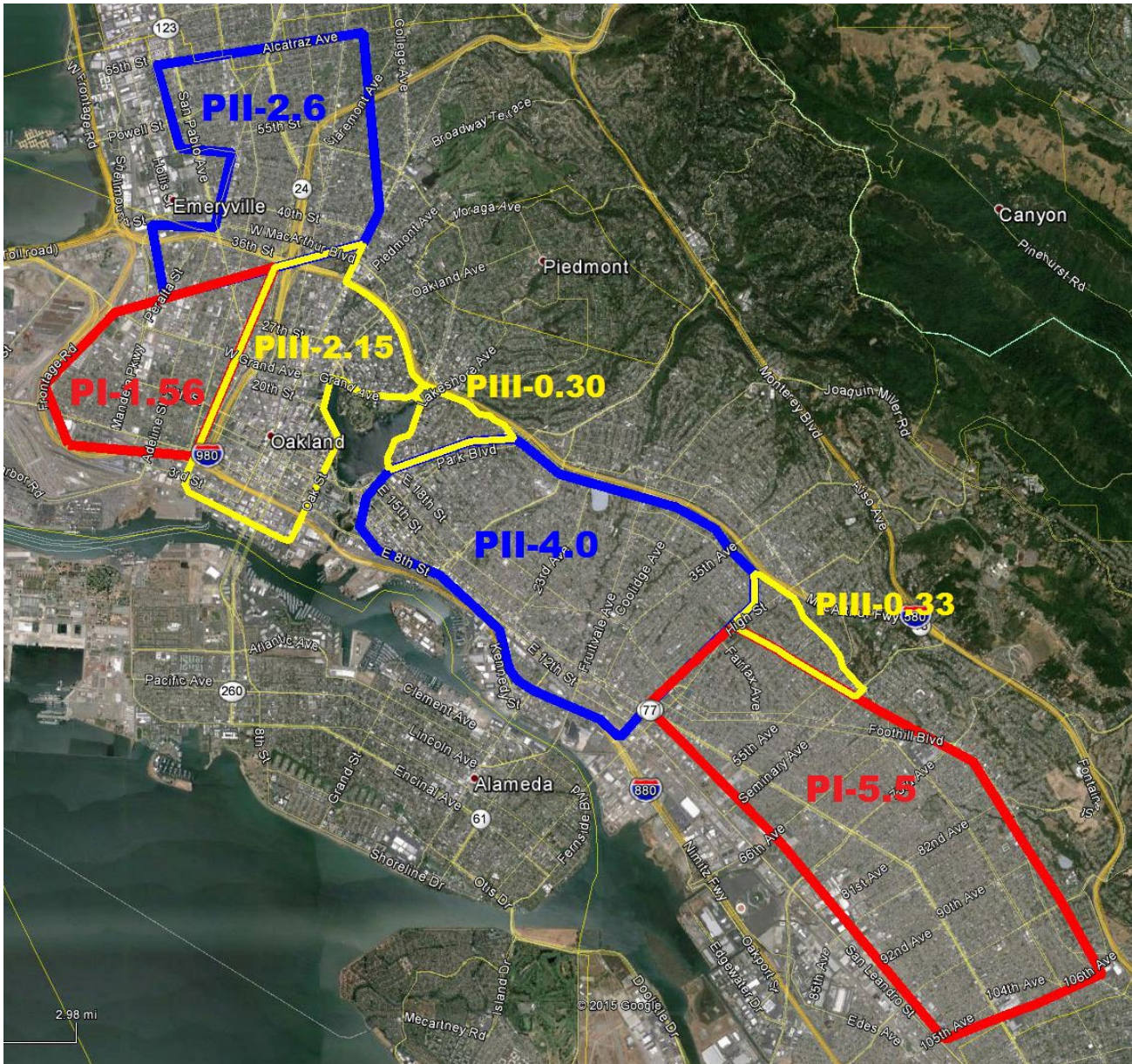
North Oakland: North of Highway 580 to Alcatraz Avenue

Phase III with yellow borders (Activated in 2016): 2.78 square miles

Downtown Oakland: Jack London Square to about West MacArthur Boulevard

Cleveland Height area: East of Lake Merritt to Highway 580 & Park Boulevard

Maxwell Park: East of High Street to Highway 580 & Mills College



* While the original contracted coverage total for Phase I was 6.0 mi², an additional 1.06 mi² of ShotSpotter coverage was added, at no charge, for a total of 7.06 mi² when Phase I service was upgraded and converted to the newer subscription platform in 2011.

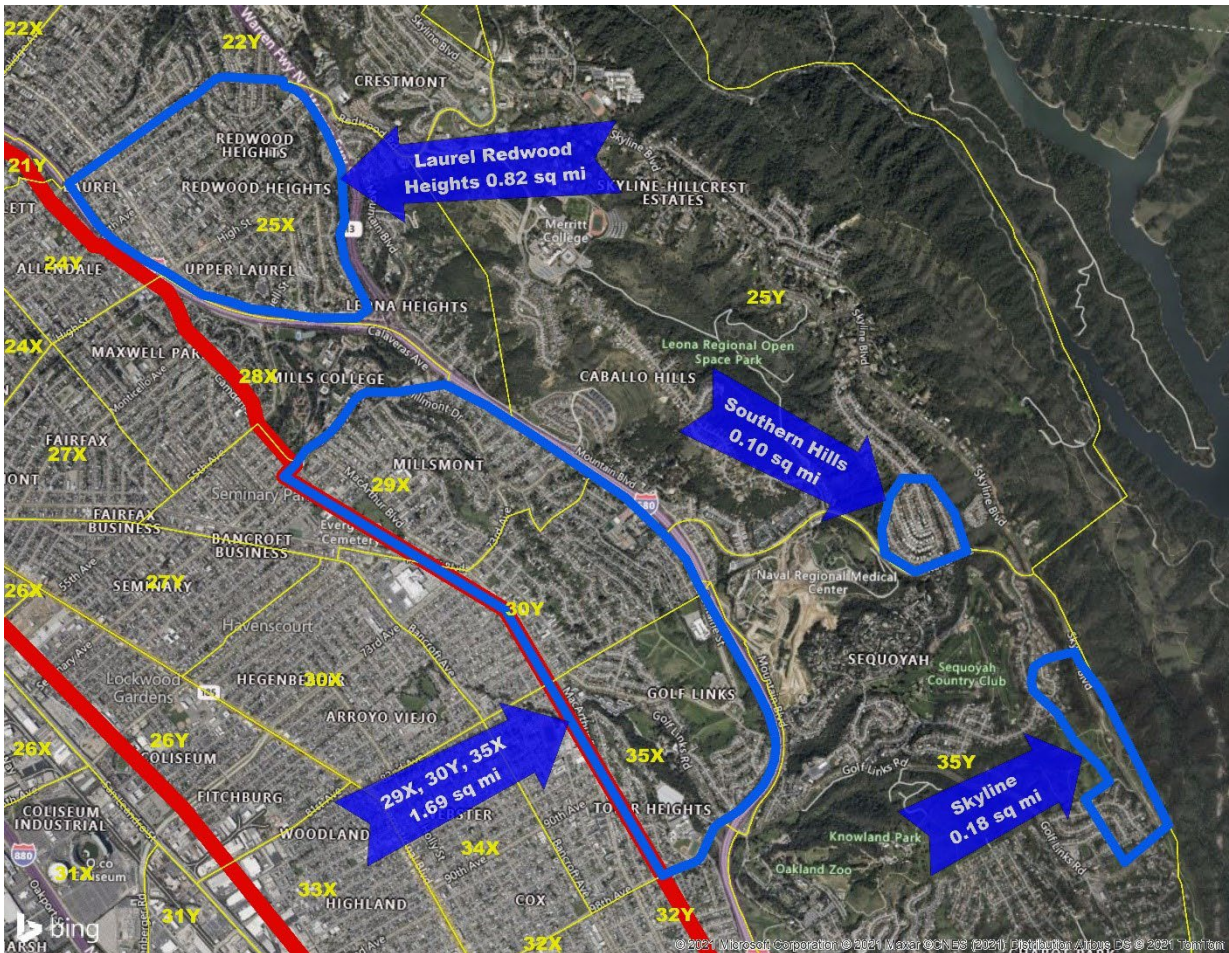
Phase IV with blue borders (Activated in 2021): 2.79 square miles

Laurel Redwood Heights: Covering a portion of Beat 25X

Southern Hills: Covering a portion of Beat 25Y

Millsmont / Golf Links: Covering Beats 29X, 30Y, and 35X

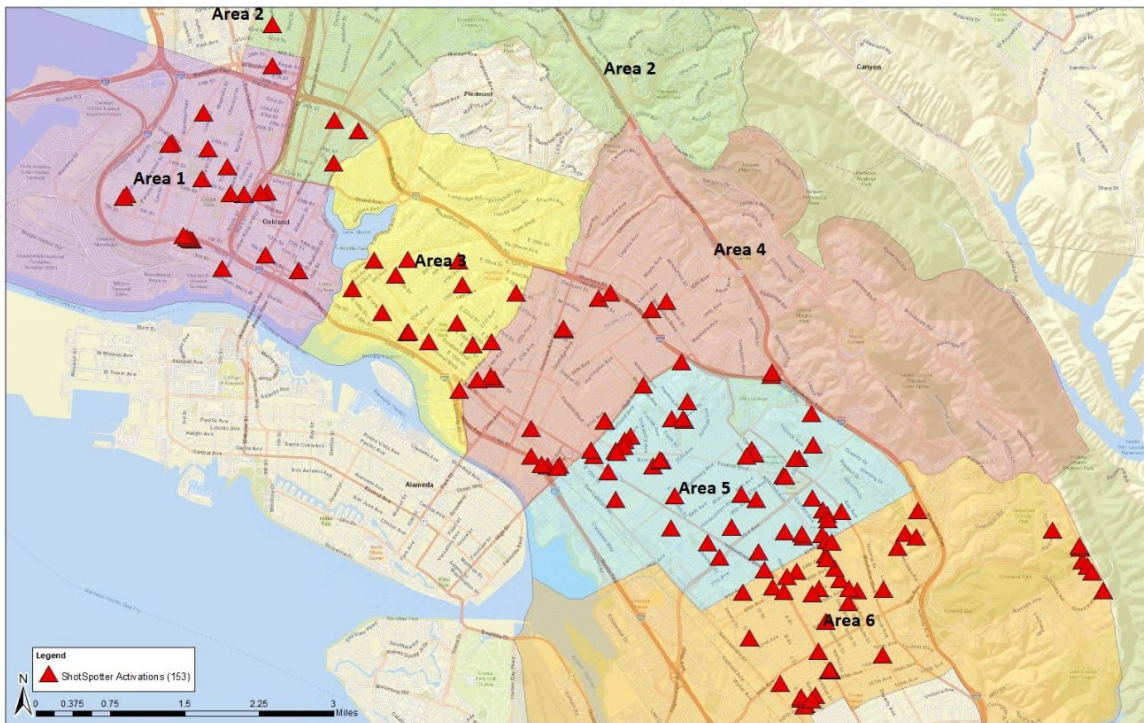
Skyline: Covering a portion of Beat 35Y





Weekly ShotSpotter Activations Report — Citywide 10 Apr. – 16 Apr., 2023

ShotSpotter Activations	Weekly Total	YTD 2021	YTD 2022	YTD 2023	YTD % Change 2022 vs. 2023	3-Year YTD Average	YTD 2023 vs. 3-Year YTD Average
Citywide	153	2,817	2,583	2,269	-12%	2,556	-11%
Area 1	20	275	270	210	-22%	252	-17%
Area 2	7	80	87	74	-15%	80	-8%
Area 3	15	287	260	250	-4%	266	-6%
Area 4	21	435	460	378	-18%	424	-11%
Area 5	46	943	754	607	-19%	768	-21%
Area 6	44	797	752	750	0%	766	-2%



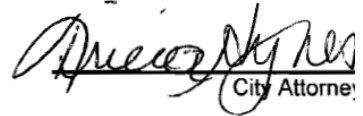
All data sourced via ShotSpotter Insight.

Produced by the Oakland Police Dept. Crime Analysis Unit.

FILED
OFFICE OF THE CITY
OAKLAND

OAKLAND CITY COUNCIL

Approved as to Form and Legality


City Attorney

2012 NOV 15 RESOLUTION No. 84119 C.M.S.

RESOLUTION:

AUTHORIZING THE CITY ADMINISTRATOR OR HER DESIGNEE TO 1) ENTER INTO AN MOU WITH THE OAKLAND HOUSING AUTHORITY (OHA) TO ESTABLISH AND DEFINE THE WORKING RELATIONSHIP AND SHARED RESPONSIBILITIES BETWEEN THE OAKLAND POLICE DEPARTMENT (OPD) AND THE OAKLAND HOUSING AUTHORITY POLICE DEPARTMENT (OHAPD). 2) ACCEPT \$150,000 FROM OHAPD FOR THE OPD FOR A JOINT PLANNED EXPANSION OF SHOTSPOTTER (SST) AND FOR OHAPD TO HAVE ACCESS TO THE SYSTEM AND ITS DATA

WHEREAS, in November 2002, OHA ended its contractual agreement with the OPD, appointing from within the department an OHAPD Chief of Police. Currently, the OHAPD has its own Chief of Police, 2 lieutenants, 6 sergeants, 25 police officers, 8 police service aides, and a communications/records supervisor. In addition to the 34 sworn staff members the Department has 10 reserve police officers; and

WHEREAS, the primary purpose of the MOU is to establish that the OPD has concurrent jurisdiction with that of the OHAPD, that OPD has primary jurisdiction throughout the City of Oakland, and that OHAPD serves as a supplemental resource. It is understood that the OPD is the primary law enforcement agency in the City of Oakland and has primary policing responsibilities in all instances; and

WHEREAS, the OHAPD's physical jurisdiction encompasses a combination of real properties owned, or under the control of the Oakland Housing Authority (OHA) contained in the City of Oakland. This includes 7 family residential developments, 5 senior citizen developments, and 267 scattered sites. In addition, OHA owns a number of administrative and maintenance facilities throughout the City of Oakland.

WHEREAS, in an effort to improve public safety and partner in innovative ways to address gun violence, the OHAPD has agreed to share the cost of the SST system and the fees associated with the expansion of the system and ongoing maintenance. The OHAPD will have access to the data and alerts generated by SST in the City of Oakland for its partnership and financial support of \$150,000 now, therefore be it

RESOLVED: That the City Council hereby authorizes the City Administrator, or her designee, to enter into a MOU with the OHAPD that outlines the responsibilities of policing in the City of Oakland and to accept \$150,000 from OHAPD to offset cost of the expansion of the ShotSpotter system and continued maintenance of the system; and be it

OPD MOU with OHAPD

Page 2

FURTHER RESOLVED: That the City Administrator or her designee is hereby authorized to complete all required negotiations, certifications, assurances, and documentation required to accept, modify, extend and/or amend the proposed MOU with OHAPD and a copy of the fully executed agreement shall be placed on file with the Office of the City Clerk; and be it

FINALLY RESOLVED: That the City Attorney shall review and approve said proposed MOU with OHAPD, as to form and legality.

DEC 4 2012

IN COUNCIL, OAKLAND, CALIFORNIA, _____

PASSED BY THE FOLLOWING VOTE:

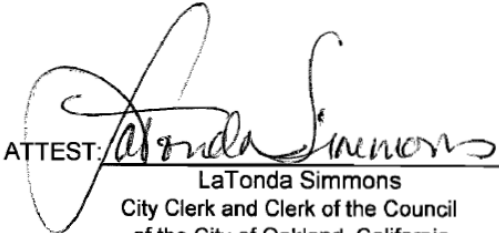
AYES - BROOKS, ~~Brunner~~, DE LA FUENTE, KAPLAN, KERNIGHAN, NADEL, SCHAAF and PRESIDENT REID - 7

NOES - 0

ABSENT - 0

ABSTENTION - 0

Excused - Brunner - 1

ATTEST: 
LaTonda Simmons
City Clerk and Clerk of the Council
of the City of Oakland, California

Attachment F: Biometric Crime Lab

Legislative History

The PAC recommended City Council adoption of the "Oakland Police Department (OPD) Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology Use Policy on October 1, 2020; following the PAC's vote, the City Council adopted Resolution No. 88388 C.M.S. on December 1, 2020. This resolution approved OPD's use of Criminalistics Laboratory DNA Instrumentation and Analysis Software Biometric Technology. In 2022, an updated Biometric Technology Use Policy and Impact Report were approved along with the required annual report adopted under Resolution No. 89458 C.M.S. filed October 20, 2022.

This memorandum is intended to serve to comply with the annual reporting mandate.

2022 Data Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

General Overview

The Oakland Police Department (OPD) Criminalistics Laboratory's (Crime Lab) Forensic Biology/DNA unit utilizes specialized DNA collection and analysis instrumentation and software to perform forensic DNA testing. During this lengthy and complicated process, one step removes and purifies DNA from cells (digestion/extraction), another quantitates how much DNA is present, and lastly, by amplifying and analyzing Short Tandem Repeats (STR) in the DNA using Polymerase Chain Reaction (PCR) and separated by Capillary Electrophoresis (CE), forensic DNA profiles are generated. Software is involved in the following processes: (i) collection and processing of STR DNA fragment data; (ii) interpretation of DNA data into DNA profiles used for comparison purposes. At the end of all processes, a determination can be made as to whether a DNA sample collected from a crime scene can be associated with a known individual through a comparison of evidentiary (crime scene) and known reference DNA profiles. Statistical weight is provided for all inclusion comparisons.

Specifics: How DNA testing was used in 2022

The Forensic Biology Unit analyzed 310 requests between January 1, 2022, to December 31, 2022. Over 1,900 items of evidence were examined, from which 4,044 samples were subjected to digestion and extraction using the Versa and EZ1 instruments. Scientist subjected 4,094 samples to quantitation analysis using the SpeedVac, Qiagility, and QuantStudio 5 instruments and 1,671 samples were subjected to amplification and typing methods using the ProFlex and 3500 instruments. The DNA profiles were processed with GMIDX or FaSTR and ArmedXpert software.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Discovery to the Alameda County District Attorney's Office was provided in 25 cases. A standard discovery packet includes the reports, technical and administrative review sheets,

case notes, attachments, contact log, resume, interpretation guidelines, photographs, electronic data, and any supporting documents.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The Biometric Use Policy covers the specific technology covered. In general, the digestion, quantitation, normalization/amplification, typing, interpretation, and databasing are housed in the laboratory of the Police Administration Building (PAB). Database equipment is located in a secure location elsewhere in the PAB, as disclosed in the Use Policy. Currently, no equipment resides outside of these locations.

A CODIS cloud-based server location is under evaluation as a replacement for the server in the PAB. The details of this location and security would be handled under the auspices of the City of Oakland ITD policy and procedure and would meet or exceed industry standards for handling secure servers.

NOTE: The use of the term "secure servers" throughout this report is on the basis of working with the Information Technology Department (ITD) in 2020 to develop terminology. ITD is responsible for the preservation, fidelity, and security of the data described herein.

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

All evidence was analyzed at the laboratory located in the PAB. No other locations are authorized. As for the geographic location of crimes, this is not collected by the laboratory in a way that can be disseminated easily. The address may be reported on the request for laboratory services form, but it is not required for analysis to proceed. The laboratory services crimes that occur in all areas of the City of Oakland.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review:

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff. The laboratory did not receive any complaints through its feedback process.

The laboratory request for services form does not collect race information. It could be argued that requiring information that is not necessary for analysis, such as race, could be biasing; indeed, it would be a great invasion of privacy to capture this data since it is irrelevant to the analyses performed. Furthermore, the race of individuals subject to the DNA analysis technology's use is not revealed during evaluation of evidence as non-coding regions of DNA are typed and do not contain this information. Therefore, staff recommends that the PAC waive the requirement to identify the race of each person subject to the technology's use and make a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the potential greater invasiveness in capturing such data.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy (SUP), and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

All Forensic Biology personnel and relevant management were required to review and sign that they understood and would abide by the Surveillance Use Policy and the Impact Reports. Under accreditation, the Laboratory actively seeks feedback from its customers, and no concerns were conveyed regarding violations or concerns around the SUP. Lastly, the Laboratory has a means to identify risks through Incident Response. Staff are encouraged to participate in Incident Response by filing Incident Alerts where there were concerns. No violations or potential violations were identified by any of these routes.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

The laboratory maintains an active security program where the security of alarmed portions of the laboratory are tested and results recorded. There were no unexplained alarm events, and there were no faults in the alarmed systems that were tested. There were no breaches to the laboratory space nor to the physical equipment that it houses. There were no identifiable data breaches or unauthorized access during the year 2022.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

The efficacy of the OPD Criminalistics Laboratory DNA analysis program is illustrated by citing the following compelling statistics:

*The laboratory completed 310 requests in 2022. These are further broken out by crime type in **Table 1** below:*

Table 1: OPD Crime Laboratory DNA Analysis Requests in 2022

Crime Type	Number of Requests
Homicide	99
Attempted Homicide	5

Rape	97
Other Sexual Assault (not rape)	24
Assault	29
Robbery	9
Burglary	6
Carjacking	4
Hit and run	1
Auto Theft	1
Weapons	29
Other Person	1
Other Criminal	3
Control Substance	2
Total	310

CODIS hits in 2022 – One hundred and forty-three DNA profiles were uploaded to the CODIS database. The laboratory had two hundred and twenty-seven associations (hits); eighty-two hits to named individuals whose identity was unknown, eleven hits to unsolved forensic cases, and sixty-four hits to previously solved forensic cases.

Thus, forensic DNA analysis is an important tool to investigate and provide potential leads for a variety of crimes that occur in the City of Oakland.

- I. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates:

There were no public record requests for DNA analysis.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Procurement of instruments is costly and is typically amortized over many budget cycles. Ongoing maintenance is imperative to ensure the reliability of the instruments is remediated quickly should a problem occur. The reagents/kits and supplies to conduct testing are also steep. The cost/benefit analysis in the form of Return on Investment (ROI) calculations place the societal cost of each homicide at \$10,000,000 and a return seen of \$135³ per dollar spent on violence reduction. Similarly, economic studies show that investigating sexual assaults results in \$81⁴ saved per dollar spent.

The total costs of procuring and maintaining the equipment are shown by Category of testing and platform below:

Digestion/Extraction

- EZ1: \$63,000 to purchase (x3 instruments = \$189,000) and \$2,990 to maintain; 3 instruments for \$8,970 annual*

³ Abt, Thomas (2019). Bleeding Out: The devastating consequences of urban violence—and a bold new plan for peace in the streets. Chapter 11, p. 208.

⁴ Wang and Wein (2018) Journal of Forensic Sciences, Analyzing Approaches to the Backlog of Untested Sexual Assault Kits in the USA, July 2018, Vol. 63, No. 4, pp. 1110-1121.

- *EZ2: \$61,250 to purchase (x2 instruments = \$122,500 and \$3,959 to maintain; 2 instruments for 7,918 annual maintenance*
- *Versa 1100: \$85,000 to purchase and \$5,000 annual maintenance*

DNA Quantitation

- *Qiagility: \$33,100 to purchase (x3 instruments = \$99,300) and \$3,433 to maintain; 3 instruments for \$10,308 annual maintenance*
- *QuantStudio 5: \$57,000 to purchase (x2 instruments = \$114,000) and \$6,280 to maintain; 2 instruments for \$12,560 annual maintenance*

DNA Normalization / Amplification

SpeedVac: \$4,000 to purchase, no maintenance

ProFlex Thermalcyclers: \$14,000 to purchase (x2 instruments = \$28,000), no maintenance

DNA Typing

3500: \$135,000 to purchase, \$11,550 annual maintenance

DNA Interpretation

STRmix: \$66,000 to upgrade, \$31,830 annual maintenance

FaSTR: \$37,000 to purchase, \$8,000 annual maintenance

ArmedExpert: \$15,000 to purchase, no maintenance

The cost of testing reagents/kits was approximately \$131,000; however, this does not include consumables such as scalpels, masks, gloves, plastics, slides, nor serological test kits.

Total purchase cost (born over several years): \$894,800

Total maintenance cost, 2022: \$96,136

Total testing cost reagents/kits, 2022: \$131,000

Estimate of consumables: \$140,000

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

The 2022 approved Surveillance Impact Report (SIR) and Biometric Technology Use Policy (SUP) were reviewed. Updates of like-for-like instrument improvements (specifically the EZ1 platform upgraded to EZ2 previously disclosed) and annual costs are included. Language about ITD's role in securing data was added to both the SIR and SUP similar to the note at the end of paragraph C above. There are no requests to substantively modify the Use Policy outside of this.

Attachment G: StarChase/GPS Tag Tracker

Oakland Police Department (OPD) Department General Order (DGO) I-22: Pursuit Mitigation System requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the Public Safety Committee. The information provided below is compliant with the annual report policy requirements of DGO I-22 as well as OMC 9.64.040.

DGO I-22 explains that “StarChase,” a private company, manufactures and supports its Pursuit Mitigation GPS Tag Tracking System. The “StarChase” system is a pursuit management technology that contains a miniature GPS tag and a launcher mounted in a police vehicle. The GPS Tag and Track Launcher System are comprised of a less-than-lethal, dual barrel GPS launcher which contains two GPS Tags (1 per barrel) mounted in the vehicle grille or on a push bumper. The launcher is equipped with compressed air and an eye-safe laser for assisting with targeting before launching the GPS Tag.

2022 Annual Report Details

- A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

GPS Tag technology was not deployed in 2022.

- B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

GPS Tag technology was not deployed in 2022.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

n/a

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

GPS Tag technology was not deployed in 2022.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the

City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

There were no audits as the technology as GPS Tag technology was not deployed in 2022.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no identifiable data breaches or unauthorized access during the year 2022.

- H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

GPS Tag technology was not deployed in 2022.

- I. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates:

There were no public records requests (open or closed) related to GPS Tag technology in 2022.

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

GPS Tag technology was not deployed in 2022 and there were zero costs.

- K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

Attachment H: Forensic Logic Coplink

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the PAC, and the Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Captain David Elzey, Criminal Investigation Division Commander, was the Program Coordinator for 2022.

2022 Annual Report Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Forensic Logic search technology is used regularly by both OPD sworn field / patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records and citations are stored:

- License plate numbers
- Persons of interest
- Locations
- Vehicle descriptions
- Incident numbers
- Offense descriptions/penal codes
- Geographic regions (e.g., Police Beats or Police Areas)

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud, and encryption of data both at rest and in transit is protected by being compliant with FIPS 140-2.

*In 2022, there were a total of 550 distinct users who conducted Forensic Logic searches, for a total of 398,386 separate queries. **Table 1** below breaks down this search data by month and by distinct user and total searches.*

Table 1: OPD CopLink Searches; by Distinct User and Search Totals – 2022

Search Type	January	February	March	April	May	June
<i>Number of OPD distinct users in each month</i>	306	316	330	299	297	311

<i>Number of searches conducted</i>	37,257	30,699	41,585	33,084	32,054	34,658
-------------------------------------	--------	--------	--------	--------	--------	--------

Search Type	July	August	September	October	November	December
<i>Number of OPD distinct users in each month</i>	300	297	324	328	315	309
<i>Number of searches conducted</i>	32,404	32,823	32,896	30,410	30,250	30,266

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Data searched with the Forensic Logic CopLink system is entirely acquired from incident reports, citations, calls for service and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other Forensic Logic client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the Forensic Logic cloud repository, it is made available to agencies subscribing to the Forensic Logic service who are permitted by their agency command staff to access CJIS information.

This is the warning message on the service user sign-on page that every user sees prior to accessing the system:

WARNING: You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures, or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report, or other information exists in the Records Management System or other law enforcement, judicial, or other information system of an identified participating agency or business.

In accordance with California Senate Bill 54, applicable federal, state, or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff.

- C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to.

The CopLink service is accessible by authorized OPD users on OPD computers with an appropriate user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include the following:

- *Arrest records*
- *Field contacts*
- *Incident reports*
- *Service calls*
- *Shots fired (ShotSpotter)*
- *Stop Data reports*
- *Traffic Accident reports*

- D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

CopLink software is not deployed in a manner as is physical hardware technology. The software is used by OPD personnel at the Police Administration Building, Eastmont Building, Communications Center, the Emergency Operations Center (when active), and in patrol vehicles to search crime incidents and related data. The data itself can relate to crime data with geographic connections to anywhere in the City, as well as the broader region and even nationally.

- E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The PAC may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the PAC makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each CopLink query. There are thousands of queries, and not all queries would provide race data of each suspect or person connected to each data result. Staff therefore recommend that the PAC makes the determination that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public benefit.

- F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

Forensic Logic conducted an audit of OPD system queries to ensure all logins were conducted by existing OPD personnel.

Forensic Logic is notified of additions or deletions to its subscription services by the designated Point of Contact at the OPD. Forensic Logic also would modify the user census upon the request of any Chief of Police, Assistant Chief of Police, or Deputy Chief of Police of the OPD.

In addition, all OPD users can only use Forensic Logic services from within OPD designated facilities such as the Police Administration Building, the Eastmont Building, the Communications Center, the Emergency Operations Center (when active), and from inside a patrol vehicle due to Forensic Logic's requirement that Internet Protocol (IP) addresses for users be whitelisted (be enabled for access). Any attempt to log in to the Forensic Logic services outside of those locations would fail by any person with an authorized OPD user ID (email address).

In addition, on an annual basis, Forensic Logic will prepare a list of enabled OPD users for review by the OPD Point of Contact to confirm that all users should be enabled for access to the Forensic Logic services. Should individuals need to be removed from the services, the Point of Contact will notify Forensic Logic at that time.

- G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no identifiable data breaches or unauthorized access during the year 2022.

- H. Information, including case examples, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Armed Robbery Series Targeting Construction Workers and Their Tools

Starting in July 2022, multiple suspects were involved in an armed robbery series where the targeted victims were construction workers and their power tools. During the investigation, the assigned Robbery Unit investigator identified one suspect. The investigator conducted a LEAP/CopLink search of the suspect's name, and several crime reports/field contact reports were located showing the suspect's previous contacts. The suspect was listed in an Oakland Police crime report as a shooting victim in 2021. A cell phone number for the then shooting victim (suspect) was listed in the crime report. A separate field contact report for the suspect listed the same cell phone number. The investigator obtained a cell phone ping warrant for the listed cell phone number associated with the suspect. The information gleaned from the cell phone ping warrant assisted in tracking the suspect and placing him on scene of two of the robberies.

There was an identified vehicle used by the suspects in their robberies. The investigator conducted a LEAP/CopLink search on the vehicle's license plate and discovered it was

associated to another suspect based on a stop data information in LEAP/CopLink. The investigator consequently connected this suspect to the suspect vehicle and one of the robbery incidents.

Home Invasion Robbery

In February 2022, three suspects committed a home invasion armed robbery. The suspects forced entry into a home, assaulted a victim, and stole property and cash. The case was assigned to a Robbery Investigator. During the investigation, one suspect (S-1) was identified by name. The investigator conducted a LEAP/CopLink search on the suspect which revealed several field contact reports where the suspect (S-1) was associated with a male subject who matched the description of one of the other suspects (S-3) provided by the victim. The investigator conducted a LEAP/CopLink search on S-3 which revealed several recent contacts throughout Alameda County where he was in a vehicle; the vehicle noted in these contacts matched the suspect vehicle that was observed on surveillance cameras at the time the home invasion robbery occurred. The victim subsequently identified S-1 and S-3 in a photo lineup. The investigator obtained arrest warrants for S-1 and S-3, and they were taken into custody.

Armed Robbery

In December 2022, three suspects committed an armed robbery of two victims. The case was assigned to a Robbery Investigator. During the investigation, it was discovered that a credit card belonging to one of the victims was used at a liquor store in Oakland. The investigator reviewed surveillance video from the liquor store capturing the date/time the stolen credit card was used. From the liquor store surveillance video, the investigator observed subjects using the stolen credit card and then enter a vehicle. The investigator conducted a LEAP/CopLink search on the vehicle, which led to the identification of one of the suspects. The LEAP/CopLink search provided information on the registered owner of the vehicle in addition to who was previously contacted operating the vehicle. Based on previous contact information involving the vehicle, the investigator connected one of those individuals as being one of the suspects involved in the robbery. The investigator subsequently obtained an arrest warrant for this suspect.

- I. Statistics and information about Public Records Act requests regarding the relevant subject surveillance technology, including response rates:

There are no existing or newly opened public records requests relating to Forensic Logic, CopLink, or LEAP (former name for CopLink).

- J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Tables 2 and 3 below provide costing data from the current Oakland Forensic Logic contract.

Table 2: Oakland Forensic Logic Contract Cost; July 2020 – June 2022

For the Period 07/01/2020 through 06/30/2022 payable upon execution of agreement:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH (07/01/20-06/30/21)	\$275	\$199	794	\$158,006	0%	\$158,006
	CopLink Analytics (07/01/20-06/30/21)	\$1,000	\$1,000	794	\$794,000	100%	\$0
	CopLink CONNECT (2 Years)	\$20,000	\$20,000	1	\$20,000	0%	\$20,000
	Integration Services NIBIN	\$5,000	\$5,000	1	\$5,000	0%	\$5,000
	Integration Services Motorola Premiere One CAD and RMS	\$25,000	\$25,000	1	\$25,000	0%	\$25,000
	CopLinkX (07/01/21-06/30/22)	\$275	\$275	794	\$218,350	0%	\$218,350
	Integration and Maintenance Services	\$25,000	\$25,000	1	\$25,000	0%	\$25,000
	Round down discount		(\$356)	1	(\$356)		(\$356)
						TOTAL	\$451,000

Table 3: Oakland Forensic Logic Contract Cost; July 2022 – June 2023

For the Period 07/01/2022 through 06/30/2023 payable on July 1 2021:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH						
	CopLink Analytics						
	CopLink CONNECT	\$10,000	\$10,000	1	\$10,000	0%	\$10,000
	CopLinkX	\$275	\$275	794	\$218,350	0%	\$218,350
	Integration and Maintenance Services	\$25,000	\$25,000	1	\$25,000	0%	\$25,000
	Round down discount		(\$350)	1	(\$350)		(\$350)
						TOTAL	\$253,000

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.